A study of open source PKI systems applicable into INDECT project

Nikolai Stoianov[1] and Emil Altimirski[2]

Abstract – **This paper provides a study of open source PKI systems applicable into European FP7 project INDECT. The requirements about type of certificates, key length and hierarchical structure are given in paper. INDECT PKI architecture with two levels of CAs are explained. Based on proposed architecture two open source PKI systems were studied: OpenCA and EJBCA. All tests were performed to create testbed that has proposed PKI architecture and covers all requirements (system and cryptographic). Finally EJBCA system was chosen for creating final INDECT PKI system.**

Keywords – **security, certificates, public-key infrastructure, PKI, cryptography.**

I. INTRODUCTION

INDECT: "Intelligent information system supporting observation, searching and detection for security of citizens in urban environment" is a Collaborative Research Project funded by the EU 7th Framework Program. Its main aim is to develop cost-effective tools for helping European Police services to enforce the law and guarantee the protection of European citizens. These tools must comply with both, country-level laws, as well as European-level directives including, among many others, the European Declaration on Human Rights [2].

A Public Key Infrastructure (PKI) is a common way to solve the problems related to the distribution of public keys, because it offers the scalability that is required for big communication and information infrastructures. A PKI is usually used to create policies, mechanisms and mechanisms for asymmetric key management, where public keys are distributed in the form of the so called digital certificates. However in INDECT the information that is included in certificates is more than just a public key since they are also employed for authentication and authorization purposes. Certificates are digitally signed to ensure the integrity and validity of the contained information [1].

II. INDECT PKI ARCHITECTURE

One of the main characteristics of the INDECT project is that is composed by multiple heterogeneous systems that exchange sensitive information among them. Therefore it is necessary to fulfill all requirements for information security: Access Control, Authentication, Non-Reputation, Data Confidentiality, Communication Security, Data Integrity, Availability and Privacy [2]. The main element of the security infrastructures being deployed to provide these security properties is the INDECT Public Key Infrastructure (PKI). This PKI is the base for creating a heterogeneous and secure environment, based on X.509 certificates, public keys and asymmetric cryptographic. The INDECT PKI architecture has a hierarchical, two-level structure [5]:

- Level I – only the Root Certification Authority (Root CA) operates at this level. This CA is offline to prevent attacks to the PKI.
- Level II – there are two CAs at this level: one for issuing certificates for users (Users CA), and other CA for issuing certificates for devices (Devices CA). Between these two CAs a trusted connection is established.

The Root CA only issues certificates for two main CAs, the Users CA and the Devices CA.

The Users CA manages (create, issue, revoke etc.) all the certificates related to the users of INDECT systems. Users use these certificates to log into the individual systems or the INDECT web portals, sign documents or encrypt connections and e-mails. These X.509 certificates can be installed in web browsers or securely stored in a smart-card.

The Devices CA manages all aspects of certificates issued for devices (PCs, PDAs, CCTVs, etc.). Each certificate is assigned to a specific device, thus each device can be uniquely identified and managed based on its certificate. Devices certificates' are used for creating secure communication channels, for signing streams and documents, and for identification.

Table 1 shows the appropriate key sizes for the proposed CA's and the certificates they issue.

TABLE 1.
SUGGESTED SIZE OF THE RSA PRIVATE KEY

CA role	Key size
Root CA	8192 bits
User CA	4096 bits
Device CA	4096 bits
User certificate	2048 bits
Device certificate	1024 bits

Figure 1 shows the different levels of the INDECT PKI and the relation between its different CAs.

[1]Nikolai Stoianov is with the C4I Development Directorate at Defence Institute, 34 Totleben Blvd, Sofia 1000, Bulgaria, E-mail: n.stoianov@di.mod.bg.

[2]Emil Altimirski is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria.

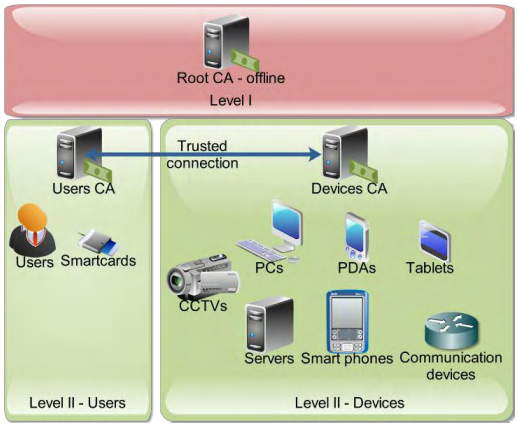

Fig. 1. Sample presentation of PKI infrastructure [5]

Digital Certificates [6]

A digital certificate is a representation of the link between the identity of a person or device and its corresponding digital information. This digital cryptographic information is comprised by the public keys of the subject. The digital certificate also contains other information related to people or devices, and this information is independently signed by the so-called Certification Authority (CA).

The basic elements of the INDECT PKI infrastructure are:

- **Root CA server** – is based on a self-signed (root) certificate, and it is always offline because it only issues the certificates of its Sub-CAs.
- **Users CA** (Subordinate certificate authority for users) – manages all certificates related to users. These certificates are stored on smart-cards to enable two-factor authentication.
- **Devices CA** (Subordinate certificate authority for devices) – manages all system certificates issued for devices. In the INDECT architecture devices could be: Servers, CCTVs, Users' PCs, Tablets, Smartphones, communication devices, etc.
- **Users RA** (Registration authority for users) - generates certificates from PKCS#10 requests, generates PKCS#12 for the end user, performs key recovery of the users‘ key (if requested using PKCS#12), edits users, revokes certificates, renews the certificates of existing users, generates a key storage for existing users, etc.
- **Devices RA** (Registration authority for devices) - generates certificates for devices, edits devices profiles, revokes certificates, renews certificates for existing devices. The Devices RA is also operated using the EJBCA software.
- **PKI Backup/Log Server** – for disaster-recovery procedures and for auditing the processes of certificate management. PKI logs are also copied into the global INDECT Audit Server.

The architecture of the deployed INDECT PKI infrastructure is shown in Figure 2.

The process for requesting and issuing certificates through a RA are as follows:

A certificate request is sent to the RA by a user.

1. The certificate request is checked and verified by the RA and stored locally.
2. The CA is waiting for certificate requests and periodically checks the RA database. It processes the request by issuing a certificate and stores it back to the RA's DB.
3. The RA periodically looks for new certificates issued by the CA.
4. The RA sends the new certificate to the user after processing it.

Certificate Revocation List (CRL)

Often some certificates must be revoked before certificates’ validity periods expire, for instance if its private key is somehow compromised. In this case the CA must create a list of revoked certificates, called Certificate Revocation List (CRL). This list includes the serial number of the revoked certificate and the reason for its revocation. Up to date information about revoked certificates is critical for a healthy PKI system. Therefore, the proposed update time for the CRLs of the INDECT PKI is 5 minutes. Four settings should be also configured on EJBCA [9] (the CA software employed for managing certificates) to define how CRL generation is done [6]:

- CRL Expire Period: This is the validity period of the generated CRL. It is set to 24 hours.
- CRL Issue Interval: This is the interval when the new CRL will be issued. For INDECT PKI it is set to 0, meaning that new CRL will be issued after old CRL is expired (24 h).
- CRL Overlap Time: This setting defines the time when the new CRL should be issued before the old CRL is expired. For INDECT PKI, the CRL Overlap Time is set to 10 minutes.
- Delta CRL Period: This setting defines the amount of time a Delta CRL (i.e. differences with a previous CRL) is valid after being issued.

Certificate extensions for INDECT users

Certificate extensions are optional by definition. This functionality was introduced in X.509 version 3. Based on these properties (extensions) it is possible to create a template and use it for issuing certificates for different purposes [1].

In INDECT peach police-officer has a unique identifier that is used for identification and stored in their certificates. The credentials of all users will be stored in LDAP repositories so for uniformity the UID (User ID) attribute is used for user identification in INDECT systems and thus this UID is also stored in certificates.

Additional information for rights management, such as the access level of users, is also stored in INDECT certificates. We assume the common security access levels: Unclassified, Restricted, Confidential, Secret and Top Secret. Therefore the certificate has an additional extension that stores the maximum access level of the user as follows:

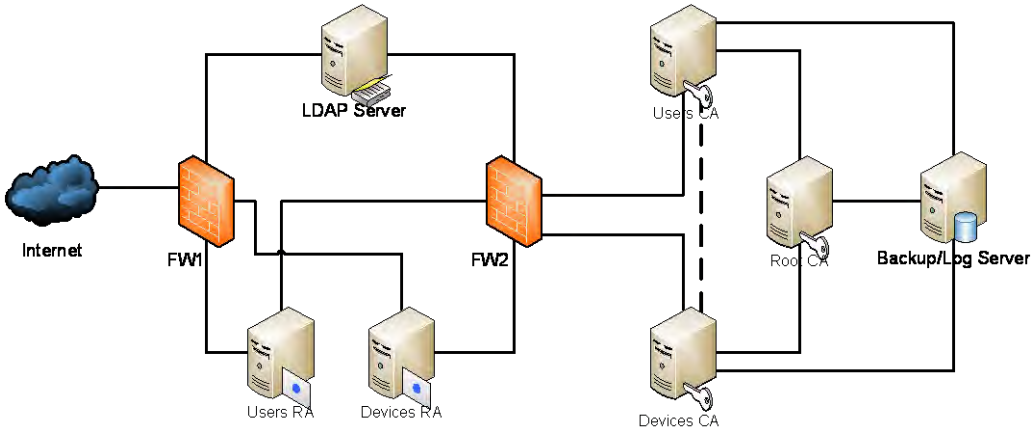

Fig. 2. Architecture of INDECT PKI [6]

- Unclassified access level: 0.
- Restricted access level: 1.
- Confidential access level: 2.
- Secret access level: 3.
- Top Secret access level: 4.

In order to test the feasibility of the proposed PKI architecture a testbed on OpenCA [3] and EJBCA [4] has been deployed.

III. OPENCA PKI SYSTEM

OpenCa project was started in 1999. Basic concepts of this PKI project is that it is consists of three parts: a Perl web interface, an OpenSSL for cryptographic operation and database for store all information needed for managing certificates and infrastructure itself.

Current version of OpenCA (OpenCA PKI v1.1.1) support following elements [3]: Public interface; LDAP interface; RA interface; CA interface; SCEP; OCSP; IP-filters for interfaces; Passphrase based login; Certificate based login; Role Based Access Control; Flexible Certificate Subjects; Flexible Certificate Extensions; PIN based revocation; Digital signature based revocation; CRL issuing.

Basic configuration consists of CA, RA and users.

To create working environment the following steps should be performed:

- Initialization of CA and database;
- Generation of new CA key and self signet certificate;
- Rebuilding CA certification chain;
- Creating and issuing RA certificate signed by CA;
- Initialization of RA;
- Issuing users' certificates.

On figure 3 sample screen shot of issuing CA certificate is shown.

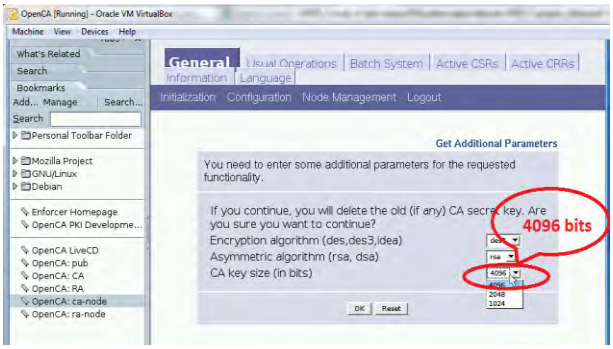

Fig. 3 OpenCA screen of issuing CA certificate

Based on OpenCA system users certificate have been issued. Sample user's certificate is shown below:

```
  Certificate:
      Data:
          Version: 3 (0x2)
          Serial Number: 4 (0x4)
          Signature Algorithm:
sha1WithRSAEncryption
          Issuer: emailAddress=nkl_stnv@tu-
sofia.bg,CN=Nikolai Stoianov,OU=WP8,O=INDECT Test
CA,C=EU
          Validity
              Not Before: Apr 11 02:08:33 2013
GMT
              Not After : Apr 10 02:08:33 2014
GMT
          Subject: serialNumber=4,CN=Nikolai
Stoianov,OU=Technical University of
Sofia,O=INDECT Test CA,C=BG
          Subject Public Key Info:
              Public Key Algorithm: rsaEncryption
              RSA Public Key: (2048 bit)
                  Modulus (2048 bit):

00:ea:7f:24:5b:a7:7f:e2:36:f6...
                  Exponent: 65537 (0x10001)
          X509v3 extensions:
              X509v3 Basic Constraints:
                  CA:FALSE
              X509v3 Certificate Policies:
                  Policy: 1.2.3.3.4
                    CPS: http://www.indect-
project.eu/cps
```

The main problem of OpenCA is that it is not possible to be issued certificate with key length more than 4096 bits.

For INDECT PKI system we define and we need certificate with key length 8192 bits. That was the reason to try to find another open source solution for creation PKI system.

IV. EJBCA PKI System

EJBCA is certification authority software that is build using Java technology. This system can be used for [4]: Strong authentication for users; Secure communication using SSL/TLS servers and clients; Smart card logon; Encrypting and signing e-mails; VPN connections; Single sign-on and etc.

Basic architecture of EJBCA PKI system consists of: CA Server; RA Server; OCSP-Responder (or LDAP cluster), MySQL database server and Separated Backup Server.

This architecture is acceptable for INDECT PKI system (see fig. 2).

Internal architecture of EJBCA has following main elements: Client; WEB; EJB and Data [4].

General concepts of EJBCA is that hierarchical infrastructure should be created. In this infrastructure RootCA has self signed certificate and it is issued certificates for SubCA and RA. SubCA is second or third level CA that manage all certificates of end entities (users and devices form IDECT point of view). Registration authorities (RA) has functionality to register all requests for new certificates and manage thrust between CAs and end entities. On figure 4 is shown screen shot for issuing RootCA certificate for INDECT Test RootCA server. As you can see maximal key length of certificate is 8192 bits that fully covers INDECT PKI requirements (see table 1).

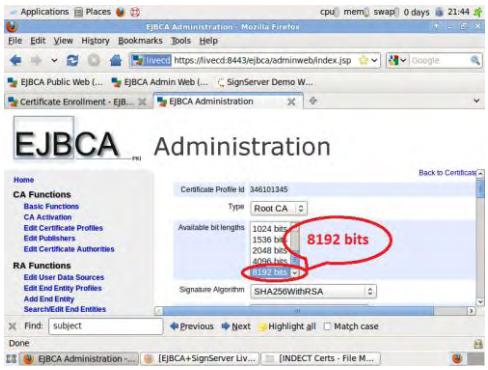

Fig. 4 Screen shot of issuing INDECT RootCA certificate

On figure 5 issued certificate of INDECT RootCA is shown. As you can see the key length of this certificate is 8192 bits.

V. Conclusion

An PKI solution for managing users' and devices' certificates is one of the preferred nowadays. Currently requirements of certificate's parameters are changing every day. This requirements should cover from one point of view all cryptographic aspects and form another point additionally all aspects of managing them including issuing, pending, revoke and etc. Two open source systems have been studied and tested - OpenCA and EJBCA. These systems have different user interface and different basic concepts for building PKI system. Limitation of OpenCA to issue certificate with keylength of 8192 bits is critical for INDECT PKI system.Based on test performed over specially created testbed we choose EJBCA for basic open source PKI systems to create INDECT PKI.

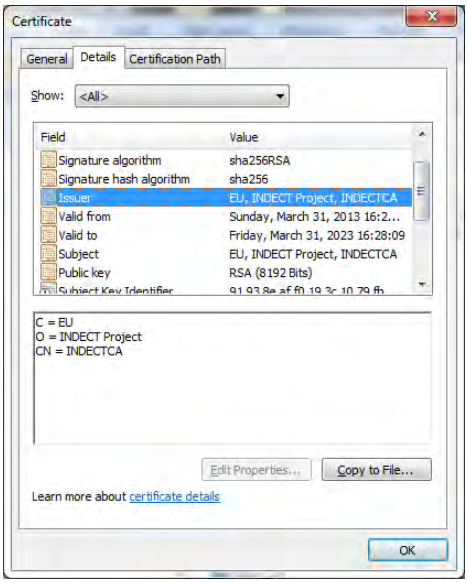

Fig. 5 INDECT RootCA certificate

Acknowledgement

This work has been funded by the EU Project INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) — grant agreement number: 218086.

References

[1] Carlisle Adams, Steve Lloyd. "Understanding PKI: Concepts, Standards, and Deployment Considerations", Second Edition, Addison Wesley, 2002, ISBN: 0-672-32391-5.

[2] INDECT project web site (2013) http://www.indect-project.eu. Accessed 30 April 2013.

[3] OpenCA project web site (2012) http://www.openca.org/. Accessed 23 April 2013.

[4] EJBCA Enterprise PKI web site (2012) http://www.ejbca.org/. Accessed 25 April 2013.

[5] Stoianov N., M. Urueña, M. Niemiec, P. Machník, G. Maestro, Security Infrastructures: Towards the INDECT System Security, MCSS 2012, CCIS 287, Springer-Verlag Berlin Heidelberg, 2012, pp. 304–315, ISBN 978-3-642-30720-1.

[6] M. Urueña, P. Machník, M. Niemiec, N. Stoianov, INDECT Security Architecture, MCSS 2013, 6-7 June 2013, AGH University, Krakow, Poland, in print.